

2151

Jakobsson 45-1-1

## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s): B.M. Jakobsson et al.  
Case: 45-1-1  
Serial No.: 09/844,121  
Filing Date: April 27, 2001  
Group: 2151  
Examiner: To Be Assigned

I hereby certify that this paper is being deposited on this date with the U.S. Postal Service as first class mail addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

Signature: Leanne M. Hanlin Date: October 26, 2001

Title: Low-Overhead Secure Information Processing for Mobile  
Gaming and Other Lightweight Device Applications

INFORMATION DISCLOSURE STATEMENT

Assistant Commissioner for Patents  
Washington, D.C. 20231

**RECEIVED**

FEB 04 2002

Technology Center 2100

Sir:

Pursuant to 37 C.F.R. §§1.56, 1.97 and 1.98, Applicants' attorney wishes to bring to the attention of the Patent and Trademark Office the following documents listed on the accompanying Form PTO-1449. A copy of each listed document is enclosed.

1. D.L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Communications of the ACM, Vol. 24, No. 2, pp. 84-88, February 1981.

2. M. Abe, "Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-servers," Eurocrypt '98, LNCS 1403, Springer-Verlag, Berlin, pp. 437-447, 1998.

3. M. Jakobsson, "Flash Mixing," Proc. of the 18th PODC, ACM Press, New York, pp. 83-89, 1999.

4. S. Goldwasser et al., "Probabilistic Encryption," Journal of Computer and System Sciences, pp. 270-299, 1984.

5. J. Katz et al., "Complete Characterization of Security Notions for Probabilistic Private-Key Encryption," Proc. of the 32nd STOC, ACM Press, New York, pp. 245-254, 2000.

6. R. Canetti, "Towards Realizing Random Oracles: Hash Functions that Hide All Partial Information," Crypto '97, LNCS 1294, Springer-Verlag, Berlin, pp. 455-469, 1997.

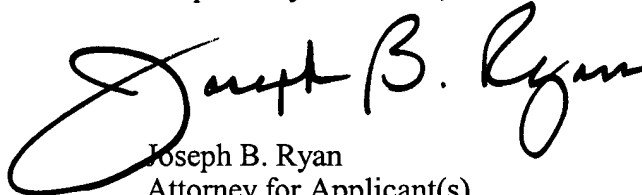
7. S. Goldwasser et al., "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks," SIAM Journal of Computing, Vol. 17, No. 2, pp. 281-308, April 1988.

8. R. Merkle, "A Certified Digital Signature," Crypto '89, LNCS 435, Springer-Verlag, Berlin, pp. 218-238, 1990.

It is believed that there is no fee due in conjunction with the filing of this Information Disclosure Statement. In the event of non-payment or improper payment of a required fee, the Commissioner is authorized to charge or to credit **Lucent Technologies Deposit Account No. 12-2325** as required to correct the error.

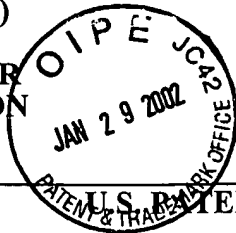
The filing of this Information Disclosure Statement shall not be construed as a representation that a search has been made, or as an admission that the information cited is considered to be material to patentability, or as a representation that no other material information exists.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Joseph B. Ryan". The signature is fluid and cursive, with a large loop at the beginning and a long, sweeping tail.

Date: October 26, 2001

Joseph B. Ryan  
Attorney for Applicant(s)  
Reg. No. 37,922  
Ryan, Mason & Lewis, LLP  
90 Forest Avenue  
Locust Valley, NY 11560  
(516) 759-7517

**FORM PTO-1449 (MODIFIED)****LIST OF PUBLICATIONS FOR  
APPLICANT'S INFORMATION  
DISCLOSURE STATEMENT**

Applicant(s): B.M. Jakobsson et al.  
Case: 45-1-1  
Serial No.: 09/844,121  
Filing Date: April 27, 2001  
Group: 2151

PATENT DOCUMENTS				
EXAMINER	DOCUMENT NO.	DATE	NAME	FILING DATE
INITIAL				IF APPROPRIATE

**FOREIGN PATENT DOCUMENTS**

EXAMINER	DOCUMENT NO.	DATE	COUNTRY	CLASS/SUBCLASS	TRANSLATION
INITIAL					YES NO

**OTHER DOCUMENTS**

EXAMINER	REF NO.	AUTHOR, TITLE, DATE, PERTINENT PAGES, ETC.
INITIAL		

1. D.L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," Communications of the ACM, Vol. 24, No. 2, pp. 84-88, February 1981.
2. M. Abe, "Universally Verifiable Mix-net with Verification Work Independent of the Number of Mix-servers," Eurocrypt '98, LNCS 1403, Springer-Verlag, Berlin, pp. 437-447, 1998.
3. M. Jakobsson, "Flash Mixing," Proc. of the 18th PODC, ACM Press, New York, pp. 83-89, 1999.
4. S. Goldwasser et al., "Probabilistic Encryption," Journal of Computer and System Sciences, pp. 270-299, 1984.
5. J. Katz et al., "Complete Characterization of Security Notions for Probabilistic Private-Key Encryption," Proc. of the 32nd STOC, ACM Press, New York, pp. 245-254, 2000.
6. R. Canetti, "Towards Realizing Random Oracles: Hash Functions that Hide All Partial Information," Crypto '97, LNCS 1294, Springer-Verlag, Berlin, pp. 455-469, 1997.
7. S. Goldwasser et al., "A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks," SIAM Journal of Computing, Vol. 17, No. 2, pp. 281-308, April 1988.
8. R. Merkle, "A Certified Digital Signature," Crypto '89, LNCS 435, Springer-Verlag, Berlin, pp. 218-238, 1990.

**RECEIVED**

FEB 04 2002

Technology Center 2100

Examiner

Date Considered

**Examiner:** Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to Applicant.